世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6
H04L 12/40, 9/00

A1

(11) 国際公開番号 WO98/48543

(43) 国際公開日 1998年10月29日(29.10.98)

(21) 国際出願番号 PCT/JP98/01837

(22) 国際出願日 1998年4月22日(22.04.98)

(30) 優先権データ
特願平9/106995 1997年4月24日(24.04.97) JP

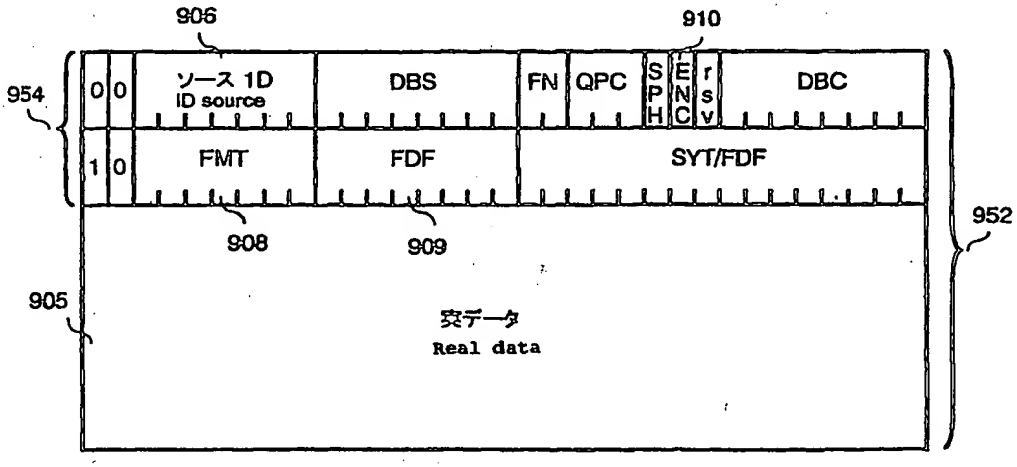
(71) 出願人（米国を除くすべての指定国について）
松下電器産業株式会社
(MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP]
〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
西村拓也(NISHIMURA, Takuya)[JP/JP]
〒576-0021 大阪府交野市妙見坂6-1-105 Osaka, (JP)
飯塚裕之(IITSUKA, Hiroyuki)[JP/JP]
〒576-0033 大阪府交野市私市6-25-6 Osaka, (JP)
山田正純(YAMADA, Masazumi)[JP/JP]
〒570-0011 大阪府守口市金田町6-24-10 Osaka, (JP)
(74) 代理人
弁理士 滝本智之, 外(TAKIMOTO, Tomoyuki et al.)
〒571-8501 大阪府門真市大字門真1006番地
松下電器産業株式会社内 Osaka, (JP)

(81) 指定国 CN, JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類
国際調査報告書

(54)Title: DATA TRANSFER METHOD

(54)発明の名称 データ転送方法



(57) Abstract

A data transfer method for preventing the malfunction of the conventional equipment which does not cope with encipherment at the time of transmitting enciphered AV information protected by a copyright through an IEEE 1394 bus. In the method, cipher identification information indicating the state of encipherment of a real data part and the real data part are contained in synchronous data transferred through isochronous communication and encipherment is effected only on the real data part. According to this method, a transmitter transmits cipher identification information indicating the state of encipherment of the real data part contained in the synchronous data together with real data and a receiver which detects the fact that the real data part has been enciphered from the cipher identification information requests the transmitter to send deciphering information and, upon receiving this information from the transmitter in response to the request, deciphers the real data part by using the deciphering information.

(57)要約

ＩＥＥＥ１３９４バスで、著作権により保護されたＡＶ情報を暗号化して送信する際に、暗号化に対応していない従来の機器も誤動作することのないデータ転送方法を提供することを目的とし、アイソクロノス通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行う。

同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データと一緒に送信装置から送信され、実データ部が暗号化されていることをこの暗号識別情報により検出した受信装置が、送信装置に対して復号化情報を要求し、この要求に従って送信装置から送信された復号化情報を受け取った受信装置はこの復号化情報を使用して実データ部の復号化を行うデータ転送方法。

明 細 書

データ転送方法

技術分野

本発明は、通常のディジタルデータと暗号化されたディジタルデータとが混在するデータを転送するディジタルデータ転送方法に関するものである。

背景技術

従来のデータ転送方式にはＩＥＥＥ１３９４規格（IEEE:THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.）を用いたデータ転送方法がある（参考文献：IEEE Std 1394:1995, High Performance Serial Bus）。ＩＥＥＥ１３９４規格におけるデータ転送には、ディジタル映像信号やディジタル音声信号等の同期データの転送に適したアイソクロノス（isochronous）通信と、制御信号等の非同期データの伝送に適したエイシンクロナス（asynchronous）通信とがあり、両方の通信はＩＥＥＥ１３９４バス上で使用することが可能である。アイソクロノス通信はいわゆる放送型の通信であり、ＩＥＥＥ１３９４バス上の１つの装置が出力するアイソクロノスパケットを、同バス上の全ての装置が受信することができる。これに対してエイシンクロナス通信には１対１の通信と１対Ｎの放送型通信の両方があり、バス上の１つの装置が出力するエイシンクロナスパケットには、そのパケットを受信すべき装置をあらわす識別子が含まれており、その識別子が特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロナスパケットを受信し、その識別子がブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロナスパケットを受信する。

また、ＩＥＥＥ１３９４規格に準拠したデータ転送方法を用いて、ディジタル音声信号やディジタル映像信号等を転送したり、ＩＥＥＥ１３９４バス上に接続された機器間でのデータ伝送を行うための規格として、ＩＥＣ（IEC: International Electrotechnical Commission 国際電気標準会議）においてＩＥＣ１８８３規格（以下、ＡＶプロトコルと称する）が検討されている。ＡＶプロトコルにおいては、映像音声データは図５に示すアイソクロノスパケット内に配置されて転送される。また、アイソクロノスパケットはＣＩＰヘッダ（CIP: Common Isochronous Packet）を含む。ＣＩＰヘッダ内には、映像音声データの種類を示す識別情報やアイソクロノスパケットを送信している送信装置の装置番号等の情報が含まれている。

図５はＡＶプロトコルにて使用されるアイソクロノスパケットのフォーマットをあらわす図である。アイソクロノスパケットは、アイソクロノスパケットヘッダ９００，ヘッダＣＲＣ９０１，アイソクロノスペイロード９０２およびデータＣＲＣ９０３からなる。アイソクロノスパケットヘッダ９００にはタグ９０７が含まれる。タグ９０７は、その値が１である時には、そのアイソクロノスパケットがＡＶプロトコルに準拠していることを示す。タグ９０７の値が１であるとき、すなわちそのアイソクロノスパケットがＡＶプロトコル準拠のアイソクロノスパケットである時には、アイソクロノスペイロード９０２の先頭にＣＩＰヘッダ９０４が含まれる。ＣＩＰヘッダ９０４の中には、当該アイソクロノスパケットを出力している出力装置の識別子であるソースＩＤ９０６が含まれる。また、ＣＩＰヘッダ９０４には、アイソクロノスペイロード９０２に含まれる実データ９０５がどの様な種類のデータであるかをあらわすＦＭＴ９０８とＦＤＦ９０９が含まれる。映像信号や音声信号のディジタルデータは実データ９０５に含まれるが、実データ９０５はアイソクロノスペイロード９０２にかならず含まれるとは限らず、パケットによっては実データ９０５を含まずにＣＩＰヘッダ９０４のみを含

むアイソクロノスペイロード９０２も有り得る。

また、ＡＶプロトコル上で機器制御を行うためのコマンド群として、ＡＶ／Ｃコマンドセットがある。（参考文献：1394 TRADE ASSOCIATION Specification for AV/C Digital Interface Command Set Version 1.0 September 13, 1996）これらのコマンドとその応答はエイシンクロナス通信を用いて転送される。

前記従来のデータ転送方法において、著作権保護のためにアイソクロノスペイロード９０２を暗号化したアイソクロノスパケットをアイソクロノス通信で送信しようとすると、暗号化されたアイソクロノスペイロード９０２の転送に対応していない従来の機器との互換性が保たれなくなる。すなわち、従来の機器は、アイソクロノスペイロード９０２の先頭にＣＩＰヘッダ９０４が正常に配置されて送信されてくることを前提に作られているので、アイソクロノスペイロード９０２が暗号化されていると、従来の機器ではＣＩＰヘッダ９０４が正常に読み出されず、そのアイソクロノスパケットはＡＶプロトコルを満たさないものと判断され、暗号化されたアイソクロノスパケットを受信した受信装置は正常に動作することができなくなる。すわなちその受信装置では実データ９０５に含まれるデータがどのような種類のデータであるかを判別することが不可能であり、当該アイソクロノスパケットを出力している装置を特定することが不可能になるので、かつ当該送信装置に対する各種の問い合わせ等のエイシンクロナス通信を行うことができなくなり、受信動作を正常に行うことが不可能となってしまうという課題があった。

また前記従来のデータ転送方法において、送信装置が出力するアイソクロノスパケットを、受信装置が継続して受信している最中にアイソクロノスパケットの暗号化が始るような場合、従来の機器においては、暗号化が始まった途端にＣＩＰヘッダ９０４を正常に読み出すことができなくなり、正常な受信が行えなくな

るという課題があった。

また送信装置が、著作権で保護されている映像音声情報等を暗号化して送信し、正規に認められた受信装置が、その暗号化された映像音声データ等を復号化するためには、送信装置は、正規の受信装置に対して復号のための復号化情報を付与する必要がある。その場合、前記従来のデータ転送方法においては、送信装置が受信装置を特定するには非常に煩雑な手順を実行せねばならない。すなわちアイソクロノスパケットには、送信を行っている装置の識別子であるソースＩＤ９０６は含まれるが、どの装置が当該アイソクロノスパケットを受信するべきかをあらわす情報は含まれておらず、そのため送信装置はどの装置が当該アイソクロノスパケットの受信を行っているかをアイソクロノスパケット送信中に調べることはできない。そこで、送信装置が、ＩＥＥＥ１３９４バス上に接続されている機器のうちのどの機器が受信を行っているかを調べるには、送信装置はバス上の全ての機器に対して受信状態の問い合わせを順次に行わねばならず、復号のための鍵情報を付与する手順が非常に煩雑になるという課題があった。

本発明は、前記従来の問題点を解決するもので、暗号化した映像音声情報をアイソクロノス通信で送信する場合にも従来の通信規格を満足し、かつ従来の受信装置が暗号化された映像音声データを含むアイソクロノスパケットを受信しても誤動作することのないデータ転送方法を実現することを目的とする。

また本発明は、前記従来の問題点を解決するもので、送信装置が正規の受信装置に復号のための鍵情報を付与する手順を極めて簡素なものにすることが可能なデータ転送方法を実現することを目的とする。

発明の開示

前記従来のデータ転送方法の問題点を解決するために、本発明のデータ転送方法においては、アイソクロノス通信で転送される同期データには実データ部の暗

号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行う。

また前記従来のデータ転送方法の問題点を解決するために、本発明のデータ転送方法においては、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データと一緒に送信装置から送信され、実データ部が暗号化されていることをこの暗号識別情報により検出した受信装置が、送信装置に対して復号化情報を要求し、この要求に従って送信装置から送信された復号化情報を受け取った受信装置はこの復号化情報を使用して実データ部の復号化を行うことによってデータ転送が行われる。

本発明のデータ転送方法においては、同期データを受信した受信装置が、同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると、送信装置に対して実データ部を復号するための復号化情報を要求する。この要求はＡＶ／Ｃセット中のコマンドによりエイシンクロナス通信を用いて行われ、この要求を受け取った送信装置においては、受け取ったコマンドのパケットヘッダを調べることにより、要求を出した機器すなわち受信装置が特定される。ここで特定された受信装置に対して送信装置が復号化情報をエイシンクロナス通信によりコマンドで付与することにより、送信装置が受信装置に復号のための復号化情報を付与する手順が極めて簡素なデータ転送方法を実現できる。

また本発明のデータ転送方法においては、同期データの暗号化は実データ部のみに対して行われ、同期データには実データ部の暗号化状況を示す暗号識別情報が含まれる。これにより、ＣＩＰヘッダは暗号化されずにそのまま転送されるので、従来の装置がこれらの暗号化された同期データを受信しても誤動作することはない。すなわち、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が暗号化された同期データを受信しても誤動作する可能性の無いデータ転送方法を実現できる。

また本発明のデータ転送においては、送信装置の送信している同期データを受信装置が継続的に受信している最中に、同期データの暗号化が始まったとしても、ＣＩＰヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

図面の簡単な説明

図１は本発明の実施形態におけるＣＩＰヘッダのフォーマットを表す模式図、

図２は本発明の実施形態における送信装置と受信装置との機能を表すブロック図、

図３Ａは本発明の実施形態におけるＡＫＥステイタスコマンドのフォーマットを表す図、

図３Ｂは本発明の実施形態におけるＡＫＥステイタスコマンドに対するＡＫＥレスポンスのフォーマットを表す図

図３Ｃは本発明の実施形態におけるＡＫＥコントロールコマンドのフォーマットを表す図

図４は本発明の実施形態における送信装置と受信装置との間で伝送されるエイシンクロナスパケットの伝送手順を表す模式図、

図５は従来のデータ転送方法におけるアイソクロノスパケットのフォーマットを表す図。

発明を実施するための最良の形態

以下、本発明の第一の実施形態について、図面を参照しながら説明する。

図１は本発明の実施形態において転送されるアイソクロノスパケットのペイロード部の形式を表した図である。本実施形態はＭＰＥＧ(Moving Picture Expert Group)に準拠したＴＳＰ（トランスポートパケット）の転送例である。

ENC（以下暗号化情報と記す）９１０は実データ９０５が暗号化されているか否かを示す。

図２は本発明の実施形態における送信装置と受信装置の関係をあらわす図である。送信装置１１０と受信装置１２８とはＩＥＥＥ１３９４バス（以下１３９４バスと記す）１１１を通じてつながれている。

先ず送信装置１１０における各ブロックの機能を以下に説明する。

信号源１００は、１３９４バス１１１上に送信しようとする１８８バイト単位のＭＰＥＧのトランスポートパケットＴＳＰ（図示せず）を暗号化手段１０１に対して出力する。すなわち本実施形態では、信号源１００は１８８バイトの固定長のデータを出力する。暗号化手段１０１は鍵生成手段１０６から与えられる暗号鍵１０９を用いて信号源１００から受け取ったＴＳＰを暗号化して出力する。本実施形態では暗号化鍵１０９が復号化情報に相当する。出力命令１０５は鍵生成手段１０６から暗号化手段１０１に対する命令であり、通常出力，暗号化出力および空出力の３種類の命令がある。出力命令１０５を受け取った暗号化手段１０１は、その命令の内容が通常出力である場合には、信号源１００から受け取ったＴＳＰをそのまま出力し、暗号化情報９１０には値０を出力する。また出力命令１０５の内容が暗号化出力である場合には、ＴＳＰを鍵生成手段１０６から受け取った暗号鍵１０９で暗号化して出力し、暗号化情報９１０には値１を出力する。また出力命令１０５の内容が空出力である場合には、信号源１００からＴＳＰを受け取るたびに空信号（図示せず）を出力するとともに、暗号化情報９１０には値１を出力する。ソースパケット化手段１０２は、暗号化手段１０１から受け取った１８８バイトのＴＳＰに４バイトのソースパケットヘッダを付加して１９２バイトのソースパケット（実データ９０５）を出力する。ＣＩＰブロック化手段１０３は、ソースパケット化手段１０２から受け取ったソースパケットにＣＩＰヘッダ９５４を付加してアイソクロノスペイロード９５２を出力する。その

際にＣＩＰブロック化手段１０３は、暗号化手段１０１から受け取った暗号化情報９１０をＣＩＰヘッダ９５４内に配置する。アイソクロノスパケット化手段１０７はＣＩＰブロック化手段１０３から受け取ったアイソクロノスペイロード９５２にアイソクロノスパケットヘッダ９００、ヘッダＣＲＣ９０１およびデータＣＲＣ９０３を付加してアイソクロノスパケットを出力する。このとき、アイソクロノスペイロード９５２の内容がＡＶプロトコルに準拠したデータであるので、タグ９０７の値は１とする。鍵生成手段１０６は、後述するように受信装置１２８との間で、図３に示すエイシンクロナスパケットのやりとりにより暗号鍵１０９を受信装置１２８に送信し、また前述のように暗号化手段１０１に対しても暗号鍵１０９を出力する。

１３９４パケット入出力手段１０８は、１３９４バス１１１と送信装置１１０との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、１３９４パケット入出力手段１０８は、アイソクロノスパケット化手段１０７から受け取ったアイソクロノスパケットおよび鍵生成手段１０６から受け取ったエイシンクロナスパケットを１３９４バス１１１上に出力するとともに、１３９４バス１１１から受信したエイシンクロナスパケットを鍵生成手段１０６へと出力する。

次に受信装置１２８の各ブロックの機能を以下に説明する。

１３９４パケット入出力手段１２７は、１３９４バス１１１と受信装置１２８との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、１３９４パケット入出力手段１２７は、１３９４バス１１１から受信したアイソクロノスパケットをペイロード抽出手段１２３に対して出力し、１３９４バス１１１から受信したエイシンクロナスパケットを鍵生成手段１２５に対して出力する。また、鍵生成手段１２５から受け取ったエイシンクロナスパケットを１３９４バス１１１に対して出力する。

ペイロード抽出手段１２３は、１３９４バス１１１から受信したアイソクロノスパケットを１３９４パケット入出力手段１２７から受取り、アイソクロノスパケットのタグ９０７の値が１である場合にはアイソクロノスペイロード９５２の中身がＡＶプロトコル準拠のデータであることを知り、アイソクロノスペイロード９５２を実データ抽出手段１２２に対して出力する。実データ抽出手段１２２は、受けとったアイソクロノスペイロード９５２に実データ９０５が含まれる場合には、アイソクロノスペイロード９５２の先頭のＣＩＰヘッダ９５４を除去した実データ９０５を復号化手段１２１に対して出力する。また、実データ抽出手段１２２は、ＣＩＰヘッダ９５４からから抽出したソースＩＤ９０６と暗号化情報９１０とを鍵生成手段１２５に対して出力する。また暗号化情報９１０は、復号化手段１２１に対しても同様に出力される。鍵生成手段１２５は、後述するように送信装置１１０との間でのエイシンクロナス通信によるエイシンクロナスパケットのやりとりにより暗号鍵１２６を受け取り、復号化手段１２１に対して暗号鍵１２６を出力する。復号化手段１２１は、実データ抽出手段１２２から受信した暗号化情報９１０の値が０の時には、実データ抽出手段１２２から受け取った実データ９０５を映像音声化手段１２０に対してそのまま出力し、暗号化情報９１０の値が１の時には、鍵生成手段１２５から受け取った暗号鍵１２６を用いて実データ９０５を復号化し、復号化した結果を映像音声化手段１２０に対して出力する。

次に前述のエイシンクロナス通信によるエイシンクロナスパケット伝送について説明する。

図３Ａ～Ｃは、エイシンクロナス通信により伝送されるエイシンクロナスパケットのフォーマットを示し、このうち図３Ａおよび図３Ｃは、本実施形態における鍵生成手段１０６と鍵生成手段１２５との間でやりとりされるＡＫＥコマンド(AKE: Authentication and Key Exchange)のコマンドフォーマットであ

り、図３Ｂはレスポンスフォーマットである。これらのコマンドおよびレスポンスは、ＡＶ／Ｃコマンドセットに属するコマンドとして、エイシンクロナス通信を用いて送信装置１１０と受信装置１２８との間でやり取りされる。これらのコマンドおよびレスポンスをやりとりすることにより、送信装置１１０および受信装置１２８の間で、相手装置の認証や暗号鍵１０９，１２６のやりとりに必要な情報の交換が行われる。前記ＡＫＥコマンドには、相手装置に対する何らかの動作を要求するＡＫＥコントロールコマンドと、相手装置の状態や能力を問い合わせるためのＡＫＥステイタスコマンドとがある。

図３ＡはＡＫＥステイタスコマンドのフォーマットをあらわす図である。ＡＫＥステイタスコマンドにおいて、オペコード２０８は、当該コマンドがＡＫＥコマンドであることを示す。アルゴリズムＩＤ２００は固定値０であり、０以外の値は将来の拡張のために予約となっている。

図３ＢはＡＫＥステイタスコマンドに対するレスポンスのフォーマットをあらわす。図３ＡのＡＫＥステイタスコマンドを受け取った装置が、そのＡＫＥステイタスコマンドを発行した装置に対して返送するのがこのレスポンスである。送信装置１１０と受信装置１２８との間で、相互認証および暗号鍵１０９、１２６の伝達を行う一連の情報交換手順には複数の種類があり、アルゴリズム領域２０１には、当該レスポンスを返す装置が実行可能な情報交換手順の識別子がビットアサインされている。すなわち、受信装置１２８は、前記の手順により暗号化されたＴＳＰを検出してから暗号鍵１０９，１２６を受け取るまでの間に、送信装置１１０との間で複数のコマンドおよびレスポンスをやり取りする。このコマンドおよびレスポンスをやり取りする情報交換手順には複数の種類があり、当該レスポンスを返す装置は、自身で実行可能な情報交換手順をアルゴリズム領域２０１における当該ビットの値を１にしてあらわす。アルゴリズム領域２０１のサイズは１６ビットであるので、最大１６種類の情報交換手順をあらわすことが可能

である。最大データ長２１２は、ＡＫＥコマンドおよびそれに対するレスポンスをやり取りする際に、受信可能な最大データ長が何バイトであるかを示す。

図３ＣはＡＫＥコントロールコマンドのフォーマットをあらわす。ＡＫＥコントロールコマンドにおけるアルゴリズム領域２０１は、アルゴリズムＩＤ２００の値が０である時には、実行中の情報交換手順をあらわす。アルゴリズム領域２０１の各ビットは、ＡＫＥコントロールコマンドおよびＡＫＥコントロールコマンドに対するレスポンスにおいては、必ず１つのビットだけが１で他のビットは０となっており、その値１の１ビットが現在実行中の情報交換手順をあらわしている。ラベル２０２は、複数のＡＫＥコントロールコマンド間の対応を明確にするために用いられる。例えば、１つの装置が他の装置に対してＡＫＥコントロールコマンドを送信したとして、そのＡＫＥコントロールコマンドを受信した装置は、受信したＡＫＥコントロールコマンドに呼応する別のＡＫＥコントロールコマンド返送するという規定が、ある情報交換手順で定められているとする。この場合、両ＡＫＥコントロールコマンド間の呼応関係を明確にするために、返送するＡＫＥコントロールコマンドに挿入されるラベル２０２は、最初に受信したＡＫＥコントロールコマンドに挿入されていたラベル２０２と同じ値を使用する。ステップ番号２０３は、情報交換手順の中でやりとりされる順に、個々のＡＫＥコントロールコマンドに対して１から順に付けられるシリアル番号である。

サブファンクション２９９は、表１に示す値をとり、この値によってそのＡＫＥコマンドの持つ意味が定まる。

表１

サブファンクション	値
メイクレスポンス	00_{16}
ベリファイミー	01_{16}
クリエイトキーインフォ	10_{16}
リコンストラクトキー	11_{16}
エクスチェンジ	20_{16}

サブファンクション２９９の内容がメイクレスポンスである場合には、当該ＡＫＥコントロールコマンドはコマンドを受信する装置に対する認証のチャレンジを意味する。このときデータ２０７には、相手の装置を認証するための乱数である認証チャレンジデータが含まれる。このコマンドを受信した装置は、サブファンクション２９９の内容をベリファイミーにしたＡＫＥコントロールコマンドを返送する。この返送の際にデータ２０７に格納されるデータは、先程受信したデータ２０７中の認証チャレンジデータに対して、あらかじめ定められた演算を行った結果である認証レスポンスデータである。この演算に使用される鍵情報は、あらかじめ正規に認定された機器にのみ付与されている鍵であるので、返送されてきた認証レスポンスデータを調べれば、演算を行った機器が正しく認定された機器であるか否かを認証することができる。

サブファンクション２９９の内容がクリエイトキーインフォである場合には、当該ＡＫＥコントロールコマンドは、このコマンドを受信する装置に対する暗号鍵１０９の要求を意味する。このＡＫＥコントロールコマンドを受け取った装置は、サブファンクション２９９の内容がリコンストラクトキーであるＡＫＥコントロールコマンドを返送する。この時、データ２０７には暗号化された暗号鍵１０９が格納されて返送される。

サブファンクション２９９の内容がエクスチェンジである場合には、当該ＡＫＥコントロールコマンドは、コマンドを送信する機器と受信する機器との間での鍵情報の交換を意味する。この鍵情報はデータ２０７に格納されて転送され、機器間の間接認証や、機器共有鍵の作成のために使用される。

表１に挙げられている以外のサブファンクションの値は将来における拡張のための予約となっている。チャネル番号２０４は、送信装置１１０と受信装置１２８との間で行うアイソクロノス通信のチャネルの番号を示す。このチャネル番号

２０４は、サブファンクション２９９の内容がクリエイトキーインフォまたはリコンストラクトキーの時にのみ有効であり、それ以外の場合にはこの値は１６進表記でＦＦとなる。ブロック番号２０５および総ブロック番号２０６は、ＡＫＥコントロールコマンドでやり取りすべきデータが一つのＡＫＥコマンドで伝送しきれない場合に使用する。すなわちこの場合には、当該データはいくつかのブロックに分割され、複数回に分けて転送される。総ブロック番号２０６は当該データを分割したブロック個数をあらわし、ブロック番号２０５は、データ２０７が幾つ目のブロックのデータであるかを示す。データ長２０９はデータ２０７に含まれる有効なデータ長をバイト数で表す。データ２０７はＡＫＥコントロールコマンドによってやり取りされるデータである。ＡＫＥコントロールコマンドを受信した装置はそのＡＫＥコントロールコマンドに対する応答を返す。その際の応答のフォーマットおよび値は、受け取ったＡＫＥコントロールコマンドのフォーマットおよび値と同じであるが、応答にはデータ２０７が含まれない点だけが唯一異なる。

図４は、送信装置１１０から受信装置１２８に対して暗号鍵１０９、１２６が送信されるまでの間に、両装置間でやり取りされるＡＶ／Ｃコマンドの具体例を時系列で模式的にあらわした図である。まず、図４に示すＡＶ／Ｃコマンドのやり取りが始まるまでの両装置の動作を簡単に説明する。

まず初期状態として、暗号化されていないＴＳＰが送信装置１１０から送信されている状況を想定する。信号源１００から出力されるＴＳＰが暗号化手段１０１に入力される。暗号化手段１０１は、出力命令１０５の内容が通常出力であるので、ＴＳＰを暗号化せずにそのままソースパケット化手段１０２へ出力するとともに、暗号化情報９１０には値０を出力する。ソースパケット化手段１０２は、受け取ったＴＳＰに４バイトのソースパケットヘッダを付加して、ＣＩＰブロック化手段１０３へ出力する。ＣＩＰブロック手段１０３は、これに８バイトのＣ

ＩＰヘッダ９５４を付加し、アイソクロノスパケット化手段１０７に対して、アイソクロノスペイロード９５２として出力する。この際、ＣＩＰヘッダ９５４に含まれる暗号化情報９１０には、暗号化手段１０１から入力した値である０をそのまま格納する。アイソクロノスパケット化手段１０７は、受け取ったアイソクロノスペイロード９５２に、アイソクロノスパケットヘッダ９００，ヘッダＣＲＣ９０１およびデータＣＲＣ９０３を付加して、アイソクロノスパケットを作成する。このアイソクロノスパケットは、１３９４パケット入出力手段１０８によって１３９４バス１１１上へ出力される。この際、当該アイソクロノスパケットがＡＶプロトコル準拠のアイソクロノスパケットであるので、アイソクロノスパケットヘッダ９００に含まれるタグ９０７の値は１となる。

信号源１００から出力されるＴＳＰが変化した時、すなわち著作権で保護されていない映像音声情報から著作権で保護されている映像音声情報へと切り替わった時、この変化を検出した鍵生成手段１０６は、出力命令１０５を通常出力から空出力へと変化させるとともに、ＴＳＰを暗号化するための暗号鍵１０９を暗号化手段１０１に渡す。

出力命令１０５の内容が空出力であるとき、暗号化手段１０１は、信号源１００からＴＳＰを受け取るたびにソースパケット化手段１０２に対して空信号を出力するとともに暗号化情報９１０に値１を出力する。暗号化手段１０１から空信号を受け取ったソースパケット化手段１０２は、ソースパケットヘッダを付加せずに、受け取った空信号をそのままＣＩＰブロック化手段１０３へと伝達する。ＣＩＰブロック化手段１０３は空信号を受け取ると、ＣＩＰヘッダ９５４だけをアイソクロノスパケット化手段１０７へ出力する。この時、ＣＩＰヘッダ９５４中の暗号化情報９１０は、暗号化手段１０１が出力した値１をそのまま用いる。アイソクロノスパケット化手段１０７は、ＣＩＰブロック化手段１０３から受け取ったＣＩＰヘッダ９５４をアイソクロノスペイロード９５２としてアイソクロ

ノスパケットを作成し、１３９４パケット入出力手段１０８へ出力する。この際、当該アイソクロノスパケットはＡＶプロトコルに準拠しているので、タグ９０７の値は1となる。１３９４パケット入出力手段１０８は受け取ったアイソクロノスパケットを１３９４バス１１１上へ出力する。当該アイソクロノスパケットは継続的に出力され、１３９４バス１１１上にはＣＩＰヘッダ９５４のみをアイソクロノスペイロード９５２に含んだアイソクロノスパケットが継続的に流れるようになる。このアイソクロノスパケットを受信した受信装置１２８では、１３９４パケット入出力手段１２７がタグ９０７を調べ、ＡＶプロトコルに準拠したアイソクロノスパケットであることを検出した後、当該アイソクロノスパケットをペイロード抽出手段１２３へ出力する。ペイロード抽出手段１２３は受け取ったアイソクロノスパケットからアイソクロノスペイロード９５２を抽出して実データ抽出手段１２２へ出力する。実データ抽出手段１２２は、ＣＩＰヘッダ９５４に含まれる暗号化情報９１０とソースＩＤ９０６とを鍵生成手段１２５へ出力する。鍵生成手段１２５は、暗号化情報９１０を調べて値が１であることを検出したのち、ソースＩＤ９０６から当該アイソクロノスパケットを出力しているのが出力装置１１０であることを知る。しかる後、鍵生成手段１２５はＡＶ／Ｃコマンドを用いて暗号鍵１０９、１２６を要求する過程、すなわち図４に示した過程へと移る。

図４において、先ずＡＫＥステイタスコマンド３００が受信装置１２８から送信装置１１０へ送信される。これにより受信装置１２８は、送信装置１１０が実行可能な情報交換手順を問い合わせることになる。これに応えて送信装置１１０はＡＫＥレスポンス３０１を受信装置１２８に対して返送する。このＡＫＥレスポンス３０１には、送信装置１１０が実行可能な情報交換手順が、アルゴリズム領域２０１内にビットアサインされており、これによって受信装置１２８は、送信装置１１０がどの情報交換手順を実行可能なのかを知ることができる。具体例

としては、送信装置１１０が実行可能な情報交換手順が第２番目のものと第６番目のものの２つであった場合には、ＡＫＥレスポンス３０１内のアルゴリズム領域２０１は２進表記で 0000000000100010 となる。

ＡＫＥレスポンス３０１を受信した受信装置１２８は、送信装置１１０が実行可能でかつ受信装置１２８自身も実行可能な情報交換手順の中から、最適な１つの手順を選択し、以降その手順にしたがってＡＶ／Ｃコマンドをやりとりする。いま仮に受信装置１２８の側で、実行可能な情報交換手順が第２番目のものと第８番目のものであった場合には、送信装置１１０および受信装置１２８の双方で実行可能な情報交換手順は、第２番目のものだけということになり、以降は第２番目の手順を用いて認証および情報の交換が行われることになる。この手順に含まれるＡＫＥコントロールコマンドでは、アルゴリズムＩＤの値が０で、アルゴリズム領域２０１の値が１６進表記で 0000000000000010 となる。情報交換手順で指定される手順には、各種ＡＫＥコントロールコマンドのやり取りの順番だけでなく、各ＡＫＥコントロールコマンドで送られるデータ２０７のフォーマットや処理方法も規定されている。

第２番目の情報交換手順に従い、鍵生成手段１２５はメイクレスポンスコマンド３０２を送信装置１１０に対して送信する。このメイクレスポンスコマンド３０２の中のデータ２０７には、鍵生成手段１２５で発生させた２つの乱数、ＲＲａとＲＲｂとが暗号化されて含まれているとともに、アルゴリズム領域２０１には第２番目の手順をあらわす識別情報が含まれている。この暗号化に際して使用する鍵は、正規に認められた送信装置と受信装置とにあらかじめ与えられている共通の秘密鍵である。メイクレスポンスコマンド３０２を受け取った鍵生成手段１０６は、受け取ったメイクレスポンスコマンド３０２のアルゴリズム領域２０１を調べて、以降は第２番目の手順を用いて認証および情報の交換を行うことを知る。鍵生成手段１０６は、第２番目の手順を実行可能なのであるから、第２番

目の手順に基づいて送信されてくるメイクレスポンスコマンド３０２のデータ２０７にはこの秘密鍵で暗号化された２つの乱数が含まれていることを知っている。そこで鍵生成手段１０６は、この秘密鍵を用いてデータ２０７からＲＲａおよびＲＲｂの２つの乱数を取り出したのち、レスポンスを作成することが可能であることを示す応答３０３を返す。しかるのち鍵生成手段１０６は、取り出した乱数のうちの一つであるＲＲａをデータ２０７に格納して、ベリファイミーコマンド３０４を受信装置１２８に対して送信する。これが先程のメイクレスポンスコマンド３０２にて要求されたレスポンスである。このベリファイミーコマンド３０４を含め、これ以降、送信装置１１０と受信装置１２８との間でやり取りされる各ＡＫＥコマンドのアルゴリズム領域２０１には全て、２番目の手順をあらわす識別情報が含まれる。

ベリファイミーコマンド３０４を受信した鍵生成手段１２５は、データ２０７の内容であるＲＲａが、自分が先程発生させた乱数ＲＲａと一致することを確かめたのち、ベリファイミーコマンド３０４に対して、正常にベリファイしたことを示す応答３０５を返す。これにより、鍵生成手段１２５は、送信装置１１０が正規に認められた送信装置であると認証する。

次に送信装置１１０は、前記メイクレスポンス３０２以降と同じ手順によって、メイクレスポンスコマンド３０６およびベリファイミーコマンド３０８を用いて、受信装置１２８が正規に認められた受信装置であることを確認する。但しこの際に使用される乱数はＲＴａおよびＲＴｂであり、ベリファイミーコマンド３０８で送り返される乱数はＲＴｂである。

この時点で送信装置１１０および受信装置１２８の双方は、乱数ＲＲｂと乱数ＲＴｂとがともにわかっていることになり、また、お互いが正規に認められた装置であることを確認したことになる。鍵生成手段１０６と鍵生成手段１２５とは、それぞれ別個に、２番目の手順で定められている共通の演算方法により、ＲＲｂ

とＲＴｂとから一時鍵（図示せず）を生成する。この一時鍵は、送信装置１１０および受信装置１２８の両装置のみが共有する共通の鍵である。

次に鍵生成手段１２５はクリエイトキーインフォコマンド３１０を送信装置１１０に対して送信する。この際、クリエイトキーインフォコマンド３１０のチャネル番号２０４には、現在受信装置１２８が受信中のアイソクロノスパケットのチャネル番号が格納される。このクリエイトキーインフォコマンド３１０を受け取った鍵生成手段１０６は、ＴＳＰの暗号化に用いる暗号鍵１０９を前記の一時鍵で暗号化したのち、クリエイトキーインフォコマンド３１０が正常に完了したことを示す応答３１１を返送する。続いて、鍵生成手段１０６は、この暗号鍵１０９を一時鍵で暗号化した結果をデータ２０７に格納したリコンストラクトキーコマンド３１２を受信装置１２８へ送る。鍵生成手段１２５は一時鍵を用いて、受け取ったリコンストラクトキーコマンド３１２のデータ２０７を復号化し、その結果暗号鍵１２６を得たのち、リコンストラクトキーコマンド３１２を正常に完了したことをあらわす応答３１３を返す。暗号鍵１０９と暗号鍵１２６とは、同じ一時鍵を用いて暗号化と復号化を行ったので、同じ鍵である。この暗号鍵１２６は鍵生成手段１２５から復号化手段１２１に対して出力される。以上の手順で復号化情報の付与が完了する。

リコンストラクトキーコマンド３１２を送信した鍵生成手段１０６は、暗号化手段１０１に対して暗号化出力を示す出力命令１０５を出力する。これを受けた暗号化手段１０１は、信号源１００から受け取るＴＳＰを暗号鍵１０９で暗号化し、ソースパケット化手段１０２への出力を開始する。これにより、１３９４バス１１１上に、暗号鍵１０９にて暗号化されたＴＳＰをアイソクロノスペイロード９５２に含むアイソクロノスパケットが送信装置１１０から送信されるようになる。受信装置１２８で受信された当該アイソクロノスパケットは、前述したように、復号化手段１２１において暗号鍵１２６を用いて復号化され、映像音声化

手段１２０へ出力される。

前記一連のＡＫＥコントロールコマンドにおいて、メイクレスポンスコマンド３０２とベリファイミーコマンド３０４，メイクレスポンスコマンド３０６とベリファイミーコマンド３０８，およびクリエイトキーインフォコマンド３１０とリコンストラクトキーコマンド３１２はそれぞれ同じラベル２０２を持つ。また、メイクレスポンスコマンド３０２，ベリファイミーコマンド３０４，メイクレスポンスコマンド３０６，ベリファイミーコマンド３０８，クリエイトキーインフォコマンド３１０およびリコンストラクトキーコマンド３１２はそれぞれ１，２，３，４，５，６なる値をステップ番号２０３に持つ。

送信装置１１０の出力するアイソクロノスパケットに含まれる実データ部１０５が、暗号化された実データ１０５から暗号化されない実データ１０５へと変化した場合には、復号化手段１２１は、暗号化情報９１０の変化を検出して復号化をやめ、実データ抽出手段１２２から受け取った出力をそのまま映像音声化手段１２０へと渡すようになる。

また、前記の図４に示した過程が始まった後に、１３９４バス１１１にバスリセットが発生した場合には、メイクレスポンスコマンド３０２以降の手順を最初からやりなおす。

以上のように本実施形態によれば、アイソクロノスパケット内の実データの暗号化状況を示す暗号化情報が実データと一緒に送信装置から送信されることにより、アイソクロノスパケットを受信した受信装置は、アイソクロノスパケット内に含まれる暗号化情報を調べ、実データが暗号化されていることを検出すると、送信装置に対して実データを復号するための暗号鍵を要求し、要求を受けた送信装置はその受信装置に対して暗号鍵を付与するので、送信装置が受信装置に復号のための暗号鍵を付与する際の手順が極めて簡素なデータ転送方法を実現できる。

また以上のように本実施形態によれば、アイソクロノス通信で転送されるアイ

ソクロノスパケットには、実データの暗号化状況を示す暗号化情報と実データとが含まれ、暗号化は実データに対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が、暗号化された実データを受信しても誤動作する可能性のないデータ転送方法を実現できる。

また以上のように本実施形態によれば、送信装置の送信している同期データを受信装置が継続的に受信している最中に、同期データの暗号化が始まったとしても、ＣＩＰヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できる。

なお，本実施形態においては、暗号鍵による暗号化が一旦開始されれば、全ての転送単位に含まれる実データは暗号化されて送信されるが、全ての転送単位に対して暗号化を行う必要はない。例えば暗号化された転送単位と暗号化されない転送単位とが交互に送信されても、ＣＩＰヘッダ中に暗号化情報が含まれているので、受信装置においては復号を正常に行うことが可能であり、同様の効果を得ることが可能である。更にこの場合、暗号化を行う転送単位の割合を受信装置が送信装置に指定しても、得られる効果が変わらないことは言うまでもない。但し、ＭＰＥＧのソースパケットはその大きさが１９２バイトであるが、ＭＥＰＧの高データレート転送（１２Ｍｂｐｓ以上）を行う際には複数のソースパケットが一つのアイソクロノスペイロードに格納される。このとき、同一のアイソクロノスペイロードの中に、暗号化されたソースパケットと暗号化されないソースパケットとの両方があってはならないことも言うまでもない。

なお、本実施形態においては、暗号鍵による暗号化は実データ部全てに対して行われたが、全ての部分に暗号化を行う必要はない。例えば、実データ部の前半分だけを暗号化したり、実データ部を４等分したうちの最初と３番目の２個所を暗号化して送信しても同様の効果が得られる。この場合は、暗号化を行った場所や割合を示す情報をＣＩＰヘッダに挿入して送信すれば、受信装置側で適切な復

号化を行うことが可能である。更に、ＣＩＰヘッダには、実データが暗号化されているか否かを示す暗号化情報のみを挿入しておき、ＣＩＰヘッダを見て暗号化されていることを検出した受信装置が、実データ部のどの部分がどのくらい暗号化されているかという情報を、エイシンクロナス通信によって送信装置に問い合わせても、同様の効果を得ることが可能である。この場合、暗号化を行う場所や割合を、受信装置が送信装置に対してエイシンクロナス通信を用いて指定しても、同様の効果が得られることは言うまでもない。また、実データ部の中でデータの重要性が高い部分についてのみ暗号化を行うと、暗号化および復号化にかかる負荷が低くなり、しかも十分な暗号化の効果が得られることも言うまでもない。

なお、本実施形態においては、送信装置と受信装置との間で相互の認証が完了するまでは実データを含まないＣＩＰヘッダのみのアイソクロノスパケットを転送したが、ＣＩＰヘッダのみのアイソクロノスパケットを出力することなく、最初から暗号化された実データを含むアイソクロノスパケットを出力しても、同様の効果が得られることは言うまでもない。

なお、本実施形態においては、送信装置と受信装置の間でやりとりされるＡＫＥコントロールコマンドの転送手順を相互の調停により決定したが、受信装置が実行可能な手順が一つだけに限られる場合にはこの調停手順をおこなわず、受信装置が実行可能な唯一の手順でコマンドの転送を開始しても同様の効果が得られることは言うまでもない。この場合には、全ての正規に認証された機器が最低限実行可能な基本手順を定めておくことが望ましい。

なお、本実施形態においては、送信装置と受信装置との間で直接認証を行い、秘密鍵による復号化情報の伝送を行ったが、認証および復号化情報の伝達手段はこれに限らない。例えば公開鍵を用いて相互に間接認証および一時鍵の作成を行ない、一時鍵を用いて復号化情報の伝送を行っても構わない。以下、その手順を簡単に説明する。

送信装置および受信装置は、相互の調停で定めた手順により、相互の間接認証に必要となる鍵情報をＡＫＥコントロールコマンドのデータ２０７に格納して送信しあう。このとき、サブファンクション２９９はエクスチェンジをあらわす。これにより、送信装置と受信装置は、互いに正規に認証された機器であれば同じ一時鍵を共有することになるので、それ以降は本実施形態と同様の手順で、クリエイトキーインフォコマンドおよびリコンストラクトキーコマンドを用いて復号化情報の伝送を行うことが可能となる。

なお、本実施形態においては、送信装置と受信装置の間でやりとりされるＡＫＥコントロールコマンドの転送手順は相互の調停により決定されたが、送信装置で実行可能な手順の種類があらかじめわかっている場合には、この調停手順をおこなわずに、送信装置の実行可能な手順で受信装置がコマンドの転送を開始しても、同様の効果が得られることは言うまでもない。

なお、本実施形態においては、送信装置と受信装置の間でやりとりされるＡＫＥコントロールコマンドの転送手順を相互の調停により決定したが、転送手順を決定する手段はこれに限らない。すなわち、複数の転送手順の個々について、あらかじめ定められた優先順位がある場合は、受信装置は、自身が実行可能な手順の中で最も優先順位の高い手順を用いて転送を開始し、送信装置がその手順を実行不能な時には、優先順位にしたがって順次次の手順を選択して転送を開始し、送信装置と受信装置の双方が実行可能な手順が見つかったならば、その手順を用いてＡＫＥコントロールコマンドの転送を行っても、同様の効果が得られることは言うまでもない。

なお、本実施形態においては、送信装置が実データ部の復号に用いる復号化情報を暗号化して、受信装置へ転送したが、受信装置が復号化情報を取得するための手段はこれに限らない。すなわち、送信装置が暗号化した復号化情報を転送するのではなく、受信装置が復号化情報を取得するのに十分な情報を送信装置が受

信装置に転送し、受信装置がこの情報から間接的に復号化情報を取得してもよい。具体的には、送信装置から受信装置へはハッシュ関数の種だけが転送され、受信装置側では受信した種をもとにハッシュ関数を用いて復号化情報を取得しても同様の効果が得られることは言うまでもない。

なお、本実施形態においては、ＡＫＥコマンドのフォーマットの一例を示したが、ＡＫＥコマンドのフォーマットはこれに限らない。すなわち、本実施形態で示したＡＫＥコマンドのフォーマットは、本実施形態を実現するための一例にすぎず、これとは異なるフォーマットのコマンドを用いても同様の効果を得ることができることは言うまでもない。

産業上の利用の可能性

以上のように、本発明のデータ転送方法では、同期データ内の実データ部の暗号化状況を示す暗号識別情報が実データ部と一緒に送信されるデータ転送が行われることにより、同期データを受信した受信装置は、同期データ内に含まれる暗号識別情報を調べ、実データ部が暗号化されていることを検出すると、送信装置に対して実データ部を復号するための復号化情報を要求し、この要求を受けた送信装置は受信装置に対して復号化情報を付与するので、送信装置が受信装置に復号のための鍵情報を付与する際の手順が極めて簡素なデータ転送方法を実現できるという優れた効果がある。

また以上のように本発明のデータ転送方法では、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、従来のデータ転送方法との互換性を保ちつつ、かつ従来の受信装置が暗号化された同期データを受信しても誤動作する可能性の無いデータ転送方法を実現できるという優れた効果がある。

また以上のように本発明のデータ転送方法では、同期通信で転送される同期データには実データ部の暗号化状況を示す暗号識別情報と実データ部とが含まれ、暗号化は実データ部に対してのみ行ってデータ転送を行うことにより、送信装置の送信している同期データを受信装置が継続的に受信している最中に同期データの暗号化が始まったとしても、ＣＩＰヘッダは暗号化されずにそのまま転送されるので、受信を行っている受信装置が誤動作する可能性のないデータ転送方法を実現できるという優れた効果がある。

また以上のように本発明のデータ転送方法では、送信装置と受信装置の間でやり取りされる認証情報および復号化情報の授受手順を送信装置と受信装置との間の調停によって選択することにより、将来の拡張性に優れた認証および復号化情報の授受手順を実現することが可能となる。すなわち、将来新しい認証方法や復号化情報が利用可能になった際に、新しい手順を使用できる機器と古い手順しか使用できない機器とが混在しても、新しい機器が古い手順を使用可能であれば、両機器間の調停により最適な手順を選択することが可能になる。すなわち本発明のデータ転送方法では、新しい機器と古い機器とが混在する環境においても、常に最適な手順を選択して実行可能になるという優れた効果がある。

また以上のように本発明のデータ転送方法では、暗号化された実データと暗号化されない実データとの割合を変化させることが可能であるので、暗号化された実データを復号するための高速処理が出来る専用ハードウェアを持たない受信装置でも、ソフトウェアによって復号化が可能になる。すなわち、パソコンのように復号用のハードウェアを持たない機器が受信装置である場合にも、暗号化される実データの割合を低下させ復号化処理を少なくすることにより、処理速度が遅いソフトウェアによる復号が可能になるという優れた効果がある。

また以上のように本発明のデータ転送方法では、送信装置と受信装置が相互に正規の機器であることを認証するまでの間は、実データを含まないアイソクロノ

スパケットを出力するので、限られたバスの転送帯域を無駄に使用することがなく、また正規に認証されていない機器が実データを受信してしまう可能性が非常に少なくなるという優れた効果がある。

請 求 の 範 囲

1．バス上の任意の機器が同期データを受信する同期（isochronousアイソクロノス）通信と、非同期データを受信する機器が特定される非同期（asynchronousエイシンクロナス）通信とが使用されるバスシステムにおいて、前記同期データは実データ部を含む場合があり、前記実データ部の暗号化状況を示す暗号識別情報が前記実データ部以外の前記同期データ中に含まれており、前記同期データを受信した受信装置は、前記実データ部が暗号化されていることを前記暗号識別情報が示している場合には、前記同期データを送信している送信装置に対して、前記非同期通信を用いて前記実データ部の復号化情報を要求し、前記要求を受けた前記送信装置は、前記非同期通信を用いて前記受信装置に対して前記実データ部の前記復号化情報を暗号化した復号化情報、もしくは前記復号化情報を取得するのに必要な復号化情報取得データを送信し、前記受信装置は、前記暗号化された復号化情報を受信した場合には、前記暗号化された復号化情報から前記復号化情報を取り出し、また、前記受信装置が前記復号化情報取得データを受信した場合には、前記復号化情報取得データを用いて前記復号化情報を取得し、このようにして得られた前記復号化情報を用いて暗号化された実データ部を復号することを特徴とするデータ転送方法。

2．前記同期データを受信した前記受信装置が、前記実データ部が暗号化されていることを検出してから前記復号化情報を取得するまでの一連の手順には、複数の種類が存在し、前記受信装置は、前記復号化情報の要求に先立って、前記送信装置が実行可能な手順の種類を前記送信装置に問い合わせ、前記受信装置は、自身と前記送信装置との双方が前記実行可能な手順の中から実行する手順を選択し、前記受信装置は選択した前記手順に基づいて前記復号化情報を取得すること特徴とする請求項１記載のデータ転送方法。

3．前記送信装置と前記受信装置との双方が前記実行可能な手順が複数存在する場合には、あらかじめ定められた優先順位に従って前記手順を選択すること特徴とする請求項２記載のデータ転送方法。

4．前記同期データを受信した前記受信装置が、前記実データ部が暗号化されていることを検出してから前記復号化情報を取得するまでの前記一連の手順には、複数の種類が存在し、前記受信装置は、前記複数の種類の手順の中からあらかじめ定められた優先順位に従って前記手順を選択して前記手順を開始し、前記受信装置の選択した前記手順を前記送信装置が実行不能である場合には、前記受信装置は、前記送信装置が実行可能な前記手順が見つかるまで、前記手順を順次選択し直して前記手順を開始し、前記受信装置は、実行可能な手順が見つかった時に、その選択した手順に基づいて前記復号化情報を取得すること特徴とする請求項１記載のデータ転送方法。

5．前記選択された手順に基づいて、前記送信装置と前記受信装置との間で授受される前記非同期データには、実行中の前記手順の種類をあらわす識別子が含まれることを特徴とする請求項２～４のいずれか記載のデータ転送方法。

6．前記受信装置は、前記復号化情報の要求を行う前に、前記送信装置が正規の送信装置であることを確認することを特徴とする請求項１～５のいずれか記載のデータ転送方法。

7．前記送信装置は、前記復号化情報の要求を受けた後、受信装置が前記正規の受信装置であることを確認してから、前記実データ部の復号化情報を暗号化して送信することを特徴とする請求項１～５のいずれか記載のデータ転送方法。

8．前記送信装置と前記受信装置とが、互いに、相手が前記正規の受信装置または前記正規の送信装置であることを確認してから、前記受信装置が前記復号化情報の要求を行うことを特徴とする請求項１～５のいずれか記載のデータ転送方法。

9．前記受信装置が前記復号化情報を要求する前に、前記受信装置から前記送信

装置に対して、前記送信装置が共通鍵を作成するのに少なくとも必要な情報の送信と、前記送信装置から前記受信装置に対して、前記受信装置が前記共通鍵を作成するのに少なくとも必要な情報の送信とが行われ、前記送信装置は前記共通鍵を用いて前記復号化情報を暗号化して送信し、前記受信装置は受信した前記暗号化された複合化情報から前記共通鍵を用いて前記復号化情報を取り出すことを特徴とする請求項１～８のいずれか記載のデータ転送方法。

１０．前記暗号化は前記実データ部に対してのみ行うことを特徴とする請求項１～５のいずれか記載のデータ転送方法。

１１．前記送信装置は内部に実データの信号源を有し、前記送信装置は前記信号源から出力された固定長単位の前記実データ毎に暗号化の有無を決定し、暗号化された前記実データと暗号化されていない前記実データとを互いに異なる前記同期通信の出力単位内に配置して前記バスシステムへ出力することを特徴とする請求項１～５のいずれか記載のデータ転送方法。

１２．前記暗号化された実データと前記暗号化されていない実データとの比率を、前記受信装置が前記送信装置に対して前記非同期通信を用いて指定し、前記送信装置は前記指定に従って暗号化の有無の比率を変更することを特徴とする請求項１１記載のデータ転送方法。

１３．前記送信装置は内部に前記実データの信号源を有し、前記送信装置は前前記信号源から出力された前記固定長単位の実データについて、前記固定長単位の実データ中での前記暗号化を行う割合を決定し、前記実データを前記同期通信の出力単位内に配置して前記バスシステムへ出力することを特徴とする請求項１～５のいずれか記載のデータ転送方法。

１４．前記受信装置は前記送信装置に対して、前記暗号化を行う割合の指定を前記非同期通信によって行い、前記送信装置は前記指定に従って前記暗号化する割合を変更することを特徴とする請求項１３記載のデータ転送方法。

１５．前記送信装置が前記同期データを送信する際に、少なくとも前記復号化情報を要求されるまでの間は前記同期データに前記実データ部を含めずに送信し、少なくとも前記復号化情報の要求を受け取った後に前記実データ部を含んだ前記同期データの送信を開始することを特徴とする請求項１～５のいずれか記載のデータ転送方法。

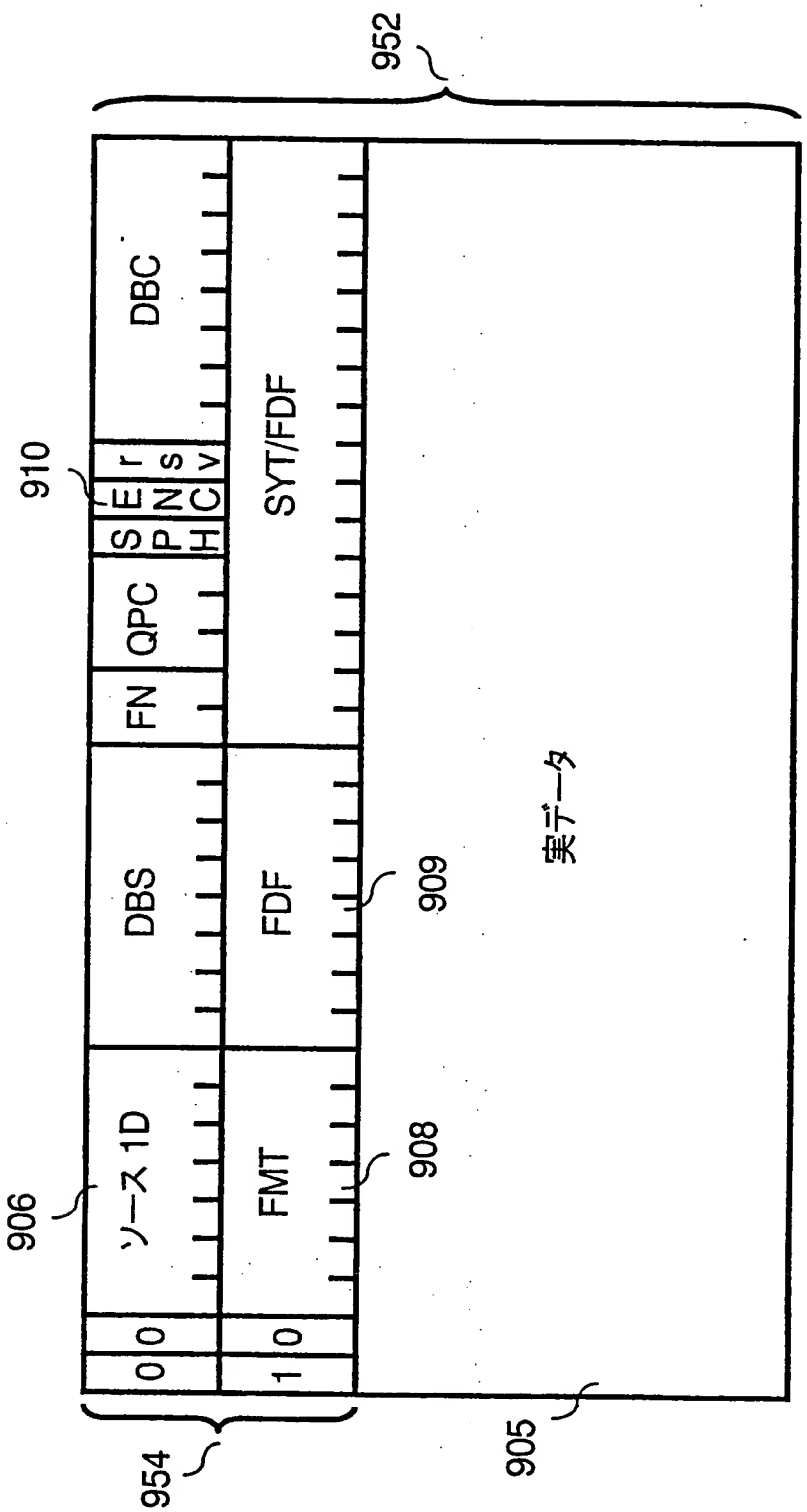


図1

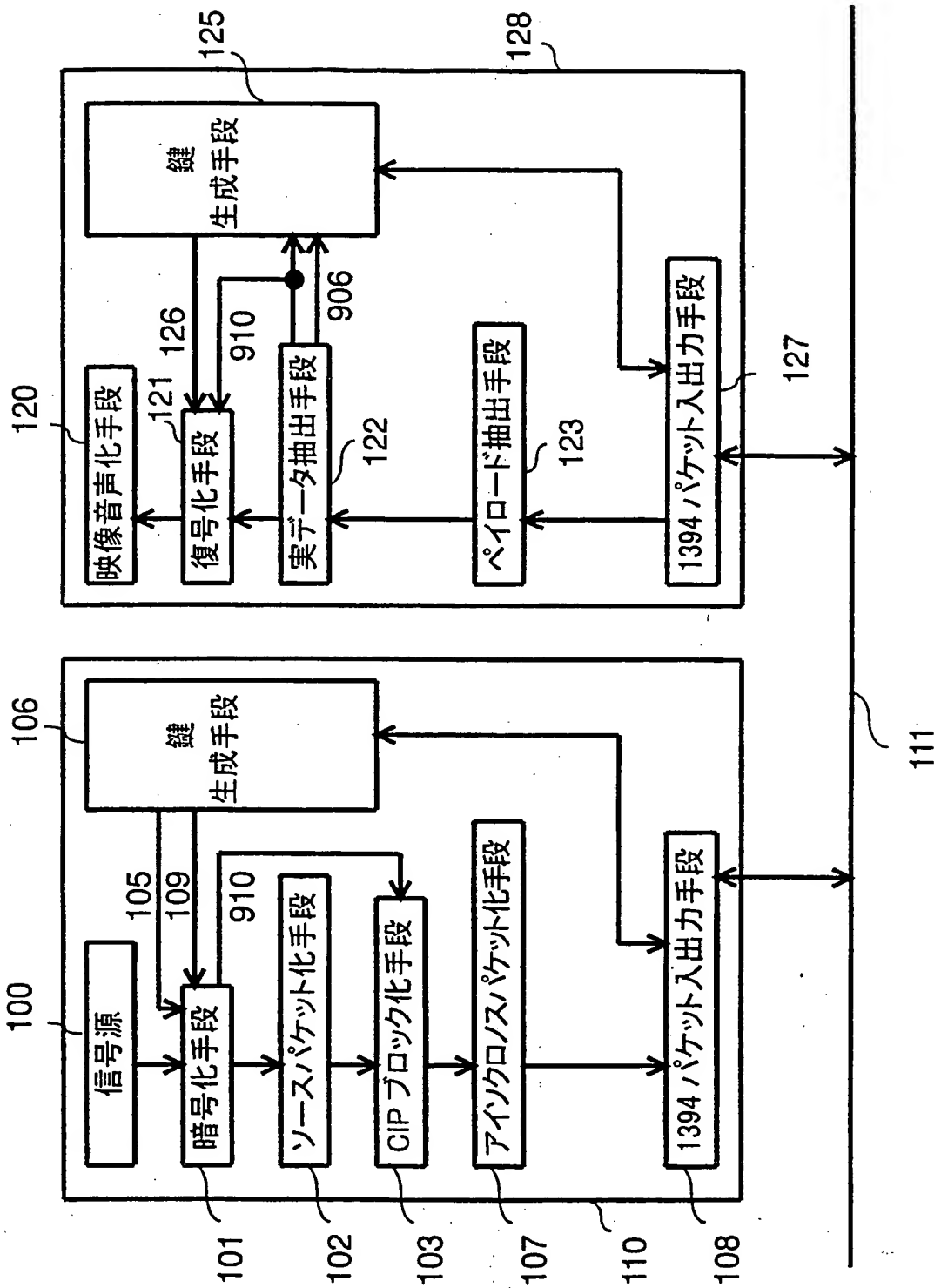

100
信号源
105
暗号化手段
101
109
910
ソースパケット化手段
102
CIP ブロック化手段
103
アイソクロノスパケット化手段
107
1394 パケット入出力手段
108
110
106
鍵
生成手段
111
120
映像音声化手段
121
復号化手段
126
910
実データ抽出手段
122
906
ペイロード抽出手段
123
1394 パケット入出力手段
127
125
鍵
生成手段
128

図 2

図３Ａ

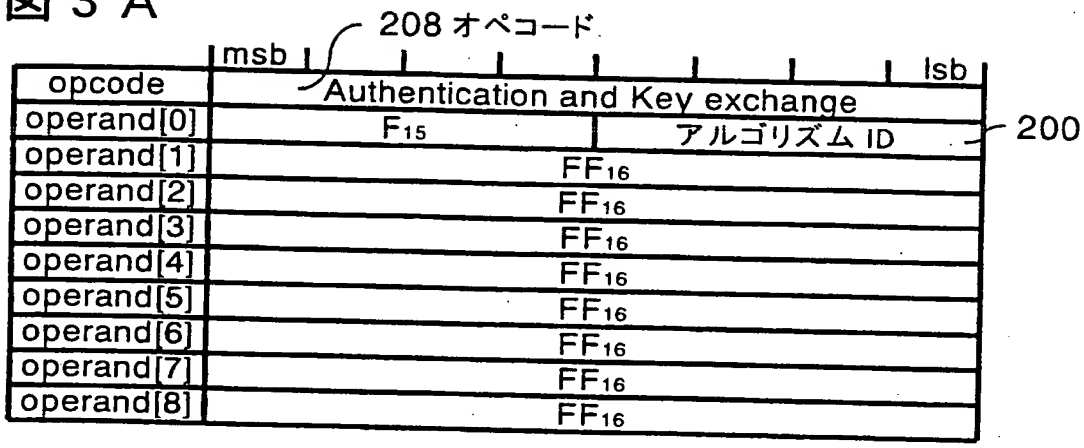


図３Ｂ

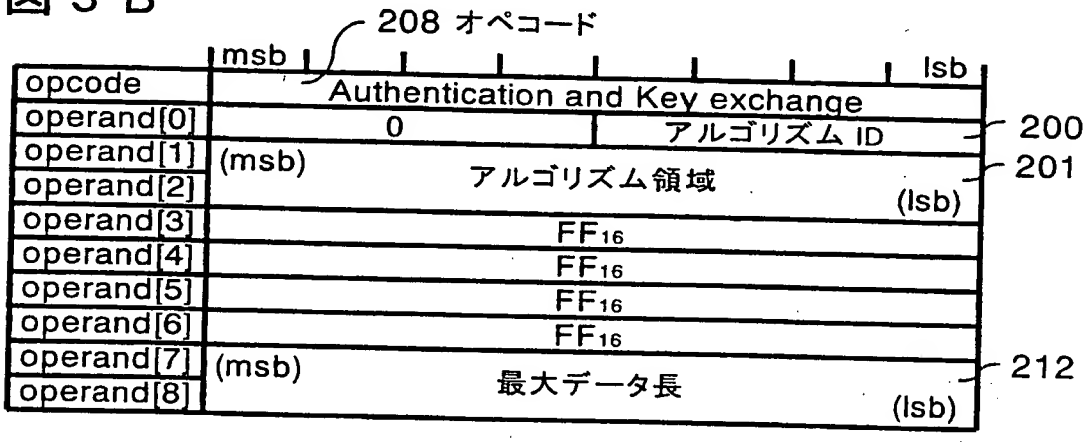
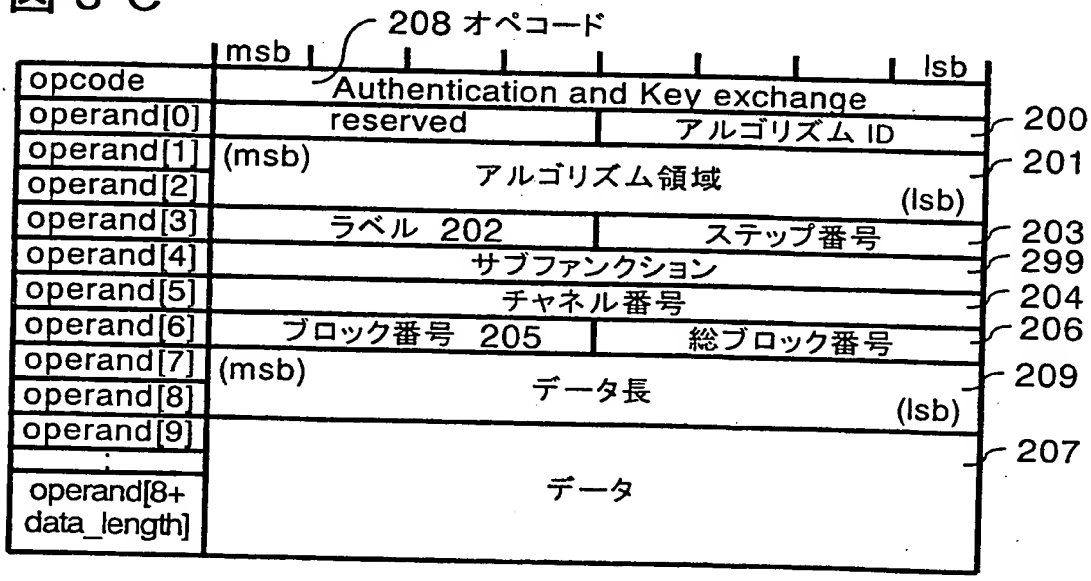


図３Ｃ



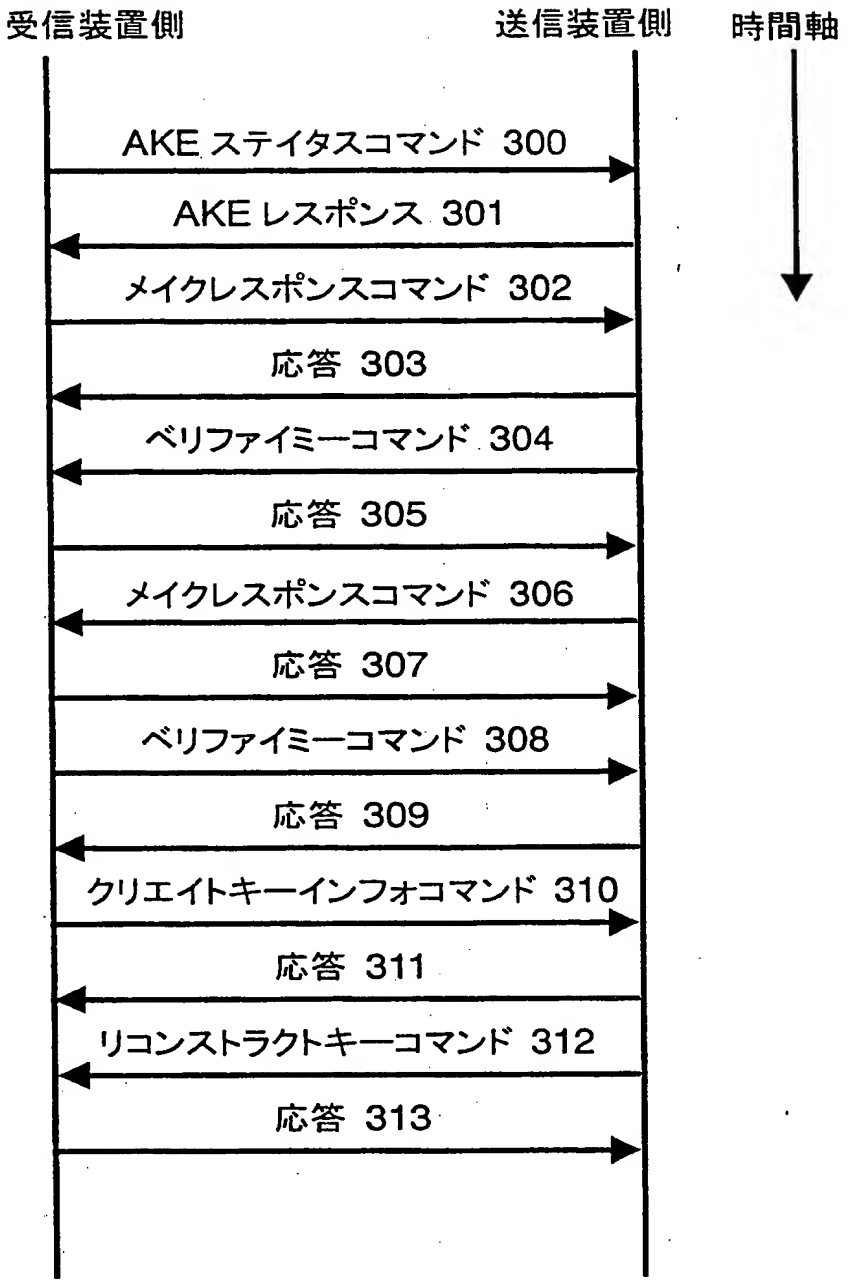

受信装置側
送信装置側
時間軸
AKE ステイタスコマンド 300
AKE レスポンス 301
メイクレスポンスコマンド 302
応答 303
ベリファイミーコマンド 304
応答 305
メイクレスポンスコマンド 306
応答 307
ベリファイミーコマンド 308
応答 309
クリエイトキーインフォコマンド 310
応答 311
リコンストラクトキーコマンド 312
応答 313

図 4

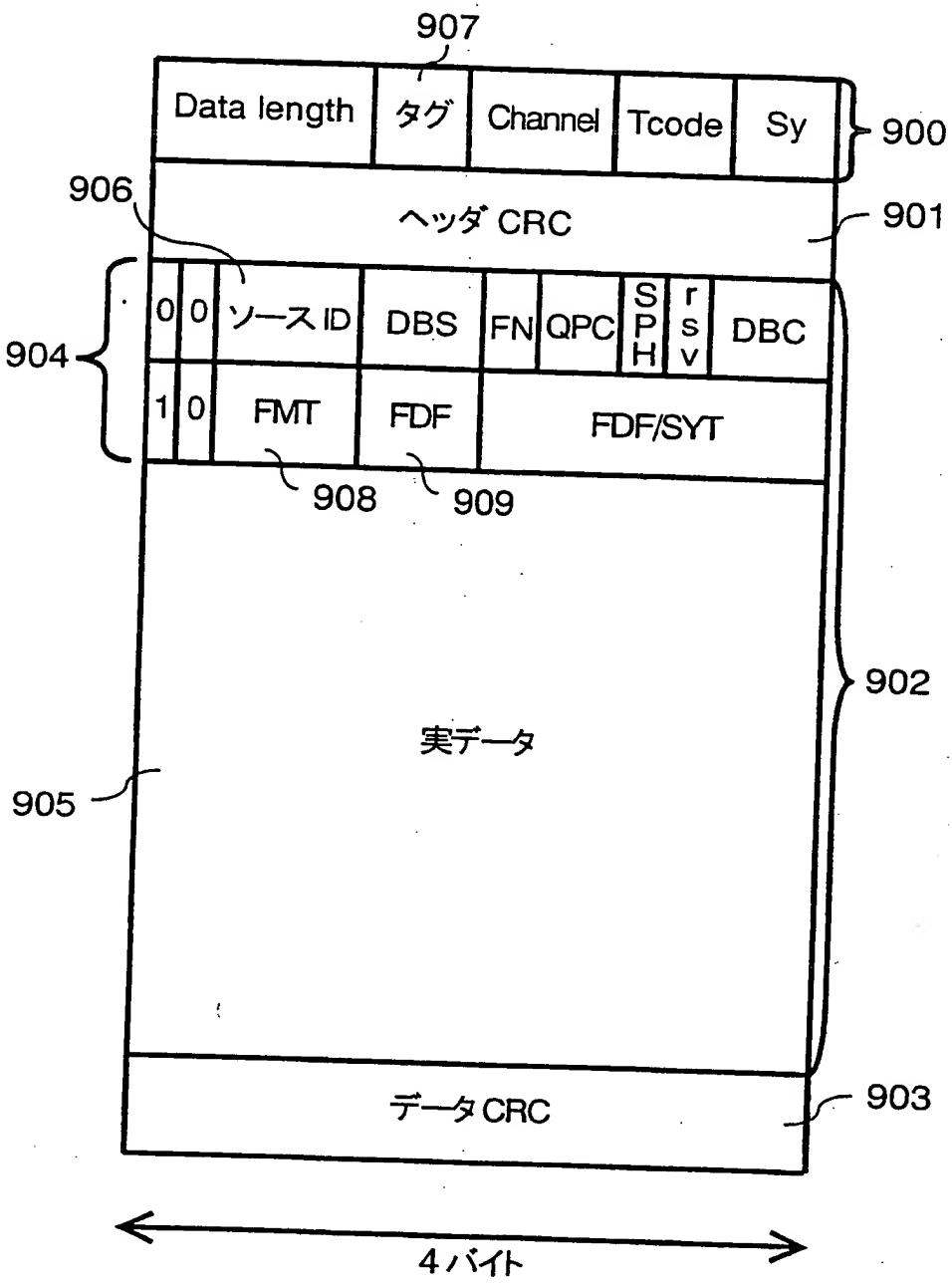


図5

図面の参照符号の一覧表

１００　信号源
１０１　暗号化手段
１０２　ソースパケット化手段
１０３　ＣＩＰぶろっく化手段
１０７　アイソクロノスパケット化手段
１０８、１２７　１３９４パケット入出力手段
１０５　出力命令
１０９、１２６　暗号鍵
１１０　送信装置
１２８　受信装置
１１１　ＩＥＥＥ１３９４バス
１０６、１２５　鍵生成手段
１２０　映像音声化手段
１２１　複合化手段
１２２　実データ抽出手段
１２３　ペイロード抽出手段
２００　アルゴリズムＩＤ
２０１　アルゴリズム領域
２０２　ラベル
２０３　ステップ番号
２０４　チャネル番号
２０５　ブロック番号
２０６　総ブロック数
２０７　データ
２０８　オペコード
２０９　データ長

２１２　最大データ長
２９９　サブファンクション
３００　ＡＫＥステイタスコマンド
３０１　ＡＫＥレスポンス
３０２、３０６　メイクレスポンスコマンド
３０３、３０５、３０７、３０９、３１１、３１３　応答
３０４、３０８　ベリファイミーコマンド
３１０　クリエイトキーインフォコマンド
３１２　リコンストラクトキーコマンド
９００　アイソクロノスパケットヘッダ
９０１　ヘッダＣＲＣ
９０２、９５２　アイソクロノスペイロード
９０３　データＣＲＣ
９０４、９５４　ＣＩＰヘッダ
９０５　実データ
９０６　ソースＩＤ
９０７　タグ
９０８　ＦＭＴ
９０９　ＦＤＦ
９１０　暗号化情報（ＥＮＣ）
９５２　アイソクロノスペイロード

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/01837

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] H04L12/40, H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] H04L12/28, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1998 Toroku Jitsuyo Shinan Koho 1994-1998
Kokai Jitsuyo Shinan Koho 1971-1998 Jitsuyo Shinan Toroku Koho 1996-1998

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 61-260735, A (Fujitsu Ltd.), November 18, 1986 (18. 11. 86) (Family: none)	1-15
A	JP, 61-81043, A (Fujitsu Ltd.), April 24, 1986 (24. 04. 86) (Family: none)	1-15
A	JP, 01-307341, A (Fujitsu Ltd.), December 12, 1989 (12. 12. 89) (Family: none)	1-15
A	JP, 01-181349, A (Nippon Telegraph & Telephone Corp.), July 19, 1989 (19. 07. 89) (Family: none)	1-15
A	JP, 09-205421, A (Canon Inc.), August 5, 1997 (05. 08. 97) (Family: none)	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
July 13, 1998 (13. 07. 98)	July 28, 1998 (28. 07. 98)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP98／01837

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl°　H04L12／40
Int. Cl°　H04L9／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl°　H04L12／28
Int. Cl°　H04L9／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926－1998年
日本国公開実用新案公報　1971－1998年
日本国登録実用新案公報　1994－1998年
日本国実用新案登録公報　1996－1998年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP, 61-260735, A（富士通株式会社）18.11月.1986（18.11.86）（ファミリーなし）	1－15
A	JP, 61-81043, A（富士通株式会社）24.4月.1986（24.04.86）（ファミリーなし）	1－15
A	JP, 01-307341, A（富士通株式会社）12.12月.1989（12.12.89）（ファミリーなし）	1－15
A	JP, 01-181349, A（日本電信電話株式会社）19.7月.1989（19.07.89）（ファミリーなし）	1－15

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」先行文献ではあるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
13.07.98	28.07.98

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	矢頭　尚之	5K	8838
	電話番号　03－3581－1101　内線　3556		

様式PCT／ISA／210（第2ページ）（1992年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９８／０１８３７

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	JP, 09-205421, A（キャノン株式会社）5.8月.1997（05.08.97）（ファミリーなし）	１－１５